

REMARKS

This amendment is responsive to the Final Office Action of December 9, 2009. Reconsideration and allowance of claims 1, 3-7, and 11-15 are requested.

The Office Action

Claims 1, 3-7, and 11-15 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Brunk et al. (USPGPUB 2002/0157005).

The Present Application

The present application is directed to an apparatus and method for authenticating an audio-visual signal by acquiring signatures from each of a plurality of blocks of an image such that the blocks may include flat or otherwise un-watermarkable content. The signatures are combined and spread throughout the entire image into regions of non-flat content. Watermarks in the regions of non-flat content are visually imperceptible, and are therefore advantageous for embedding.

The References of Record

Brunk et al. discloses calculating a metric of an embedded digital watermark and embedding the watermark into a media signal. Mid- and high-frequency Fourier coefficients are weighted then inverse transformed to generate a watermarked image.

The Claims Are Not Anticipated By Brunk et al.

Claim 1 calls for dividing a whole image, that contains at least one flat region, into a plurality of regions. Signatures bits are generated from each of the regions, including a region which contains flat content. The signature bits are included in a signature which is embedded across a portion of the image that is larger than one of the regions. The signature is embedded such that the signature bits, included in the signature, can be extracted even if the region with flat content has been replaced by tampering and thus the image is protected from tampering in the region of flat content.

In contrast, Brunk does not spread the signature bits throughout the image, but Fourier coefficients spread symmetrical about the vertical and/or horizontal axes are selected to be weighted according to a pre-defined reference value (§ 20). Furthermore, Brunk discloses that the calibration impulses are embedded back into the block where derived from (§ 25, lines 15-16). The problem with the Brunk approach is that if signature bits are embedded back into the blocks where they are derived from, the generated signature bits from flat content do not carry a sufficient payload to detect tampering. In order to maintain invisibility in flat regions, the generated signature bits cannot be reliably embedded. Hence, when a flat region has no embedded signature, it will not be known whether the signature error is due to tampering or the original content being flat. Consequently, the Brunk method cannot determine whether flat content has been tampered with or not.

Brunk does disclose that “the fragile watermark may be spatially replicated in contiguous blocks of the image” (§ 92, lines 6-7). First, the fragile watermark is merely for copy detection, not tamper detection. This is, as described in the present specification on page 3, paragraph 2, as “backup embedding” where the embedding location has as fixed spatial relation to the original embedding. If the contiguous blocks are composed of flat content, then the payload of the watermark will not be strong enough to ensure degradation is the result of tampering. Thus, signature bits cannot be extracted when authenticated the image. Consequently, the Brunk fragile watermark cannot be embedded in only non-flat content because the detector must isolate the spatial location of the tampering (§ 92). Therefore the watermark must be embedded according to location and not flat versus non-flat content.

Claim 11 further calls for embedding the signature across more than one block (1) without subdividing the signature and (2) leaving the lat area unchanged.

In contrast, Brunk embeds the signature back into each block and in § 92 replicates the signature into contiguous blocks. In § 71, Brunk repeats the signature in temporally contiguous blocks, i.e. the same block of a subsequent frame. Embedding the signature in flat regions causes visible changes in the image. Failing to imbed the signature in another block which is flat opens the door for tampering.

Brunk fails to recognize that the solution to this conundrum is to spread the signature without subdividing over plural blocks.

Additionally, Brunk only selects M coefficients, which are only in the mid- to high-frequency range, to contribute to the watermark. A block with predominately flat content, i.e. coefficients in the low frequency range, will not contribute to the watermark.

Claim 11 calls for computer-executable instructions which include a second module which generates a signature where each block contributes at least one bit of the signature.

In contrast, Brunk performs frequency transform and inverse transform for each block, but only M coefficients are selected to contribute to the watermark (§ 20-23). Therefore each block does not necessarily contribute to one bit of the signature. Since the coefficients are only in the mid- to high-frequency ranges, then a block with flat content, i.e. low frequency, will not contribute to the watermark.

Claim 14 calls for receiving at least one video image with a processor. The processor divides the image into a plurality of regions including at least one region of flat content and a plurality of regions of non-flat content. At least one of bit of a signature is generated from each of the regions including the at least one non-flat region. The signature is then embedded only in the plurality of regions with non-flat content.

Brunk does disclose that “the fragile watermark may be spatially replicated in contiguous blocks of the image” (§ 92, lines 6-7). However, Brunk does not make the distinction that the contiguous blocks include only non-flat content. This is, as described in the present specification on page 3, paragraph 2, as “backup embedding” where the embedding location has as fixed spatial relation to the original embedding. If the contiguous blocks are composed of flat content, then the payload of the watermark will not be strong enough to ensure degradation is the result of tampering. Thus, signature bits cannot be extracted when authenticated the image. Consequently, the Brunk fragile watermark cannot be embedded in only non-flat content because the detector must isolate the spatial location of the tampering (§ 92). Therefore the watermark must be embedded according to location and not flat versus

non-flat content. The same problem arise in ¶ 71 when the signature is replicated in temporally contiguous blocks, i.e. the same blocks of subsequent frames.

If the watermark image does undergo a transformation, such as digital-to-analog conversion, printing, photocopying, scanning, analog-to-digital conversion, ect., the watermarked image will not corrupt in a predictable manner as is required for the Brunk method to succeed (¶ 25).

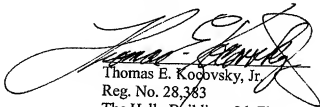
CONCLUSION

For the reasons set forth above, it is submitted that claims 1, 3-7, and 11-15 (all claims) distinguish patentably over the references of record and meet all statutory requirements. An early allowance of all claims is requested.

In the event the Examiner considers personal contact advantageous to the disposition of this case, the Examiner is requested to telephone Thomas E. Kocovsky, Jr. at 216.363.9000.

Respectfully submitted,

Fay Sharpe LLP

A handwritten signature in black ink, appearing to read "Thomas E. Kocovsky, Jr.", is written over a horizontal line.

Thomas E. Kocovsky, Jr.
Reg. No. 28,383
The Halle Building, 5th Floor
1228 Euclid Avenue
Cleveland, OH 44115-1843
216.363.9000